Math. Commun. **26**(2021), 151–158

Cyclic abelian varieties over finite fields in ordinary isogeny classes

Alejandro J. Giangreco-Maidana*

Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, 13453 Marseille, France

Received May 4, 2020; accepted February 17, 2021

Abstract. Given an abelian variety A defined over a finite field k, we say that A is *cyclic* if its group $A(k)$ of rational points is cyclic. In this paper, we give a bijection between cyclic abelian varieties of an ordinary isogeny class $\mathcal{A}$ with Weil polynomial $f_{\mathcal{A}}$ and some classes of matrices with integer coefficients and having $f_{\mathcal{A}}$ as a characteristic polynomial.
AMS subject classifications: 11G10, 14G15, 14K15

Key words: group of rational points, cyclic, ordinary abelian variety, finite field, isogeny class, class of matrices

1. Introduction

The group $A(k)$ of rational points of an abelian variety A defined over a finite field $k = \mathbb{F}_q$ is a finite abelian group, and it has theoretical and practical interests. More precisely, the group structure of $A(k)$ and some statistics are research topics in the literature.

The structure of all possible groups for elliptic curves defined over finite fields was independently discovered in [12], [10],[15] and [18]. For higher dimensions, in [11] Rybakov gives a very explicit description of all possible groups of rational points of an abelian variety in a given isogeny class with commutative endomorphism algebra. His result is formulated in terms of the characteristic polynomial of the isogeny class.

Cyclic subgroups of the group $A(k)$ of rational points of an abelian variety A defined over a finite field k are suitable for multiple applications, in particular for cryptography, where the Discrete Logarithm Problem is exploited. We say that an abelian variety A is *cyclic* if its group $A(k)$ of rational points is cyclic. Vlăduţ studied the cyclicity of elliptic curves in [16] and [17]. The higher dimensional case was studied by the author in [4] and [5], when varieties are grouped in their isogeny classes.

Deligne's functor ([2]) describes an equivalence of categories between ordinary abelian varieties and modules over $\mathbb{Z}$ with certain properties. A classical result of Latimer and MacDuffee gives a bijection between certain classes of matrices with integer coefficients and certain classes of fractional ideals (see [7]). Combining these two results with a criterion for cyclic varieties based on their endomorphisms rings, we obtain our main result.

*Corresponding author. *Email address:* ajgiangreco@gmail.com (A. J. Giangreco-Maidana)

Recently, a lot of effort has been done on the computational aspects of abelian varieties (see for example [8] or the LMFDB project [3]). Besides theoretical interests, our work could contribute to the computation of the group structure of varieties.

2. Preliminaries and statement of the result

Abelian varieties over finite fields

For the general theory of abelian varieties, see for example [9], and for precise results over finite fields, see [19].

Let $q = p^r$ be a power of a prime, and let $k = \mathbb{F}_q$ be a finite field with q elements. Let A be an abelian variety of dimension g over k. For an extension field K of k, we denote by $\mathrm{End}_K(A)$ the ring of K-endomorphism of A and by $\mathrm{End}_K^0(A)$ its endomorphism algebra $\mathrm{End}_K(A) \otimes \mathbb{Q}$. Abelian varieties belonging to the same isogeny class have isomorphic endomorphism algebras. For an integer n, denote by $A[n]$ the group of n-torsion points of $A(\overline{k})$. It is known that

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}, p \nmid n; \text{ and,}$$
$$A[p] \cong (\mathbb{Z}/p\mathbb{Z})^i, 0 \leq i \leq g.$$

For a fixed prime ℓ ($\neq p$), $A[\ell^n]$ form an inverse limit system under $A[\ell^{n+1}] \xrightarrow{\ell} A[\ell^n]$, and we can define the *Tate module* $T_\ell(A)$ by $\varprojlim A[\ell^n](\overline{k})$. This is a free $\mathbb{Z}_\ell$-module of rank $2g$ and the absolute Galois group $\mathcal{G}$ of $\overline{k}$ over k operates thereon by $\mathbb{Z}_\ell$-linear maps.

The Frobenius endomorphism F of A acts on $T_\ell(A)$ by a semisimple linear operator, and its characteristic polynomial $f_A(t)$ is called the *Weil polynomial of* A (also called the *characteristic polynomial of* A). The Weil polynomial is independent of the choice of the prime ℓ. A monic polynomial with integer coefficients and all its roots having absolute value $\sqrt{q}$ is called a *q-Weil polynomial*. Note that a q-Weil polynomial of degree $2g$ has q^g as a constant term. Weil proved that the characteristic polynomial of A is a q-Weil polynomial. Nevertheless, not every q-Weil polynomial is the characteristic polynomial of an abelian variety.

In [13], Tate proved that two abelian varieties A and B are isogenous if and only if $f_A = f_B$. Thus, it makes sense to consider the Weil polynomial $f_{\mathcal{A}}$ of an isogeny class $\mathcal{A}$ as being the Weil polynomial of some (and thus any) abelian variety of $\mathcal{A}$. Moreover, the Honda-Tate theory gives a bijection between irreducible q-Weil polynomials and simple isogeny classes. If A is simple, $f_A(t) = h_A(t)^e$ for some irreducible q-Weil polynomial h_A and the center of $\mathrm{End}_k^0(A)$ is isomorphic to the number field $\mathbb{Q}(F) \cong \mathbb{Q}[t]/(h_A(t))$. The cardinality of the group $A(k)$ of rational points of A equals $f_A(1)$, and thus, it is an invariant of the isogeny class.

An abelian variety A is *ordinary* if one of the following equivalent conditions is satisfied:

1. A has p^g points of order dividing p and defined over $\overline{k}$;
2. The neutral component of the group scheme A_p, the kernel of multiplication by p, is of multiplicative type;

3. At least half of the roots of f_A are p-adic unities.

It follows from 3 that being ordinary is a property of the isogeny class. The characteristic polynomial of an ordinary simple abelian variety is irreducible ([6, Th. 3.3]).

Matrices

Let us define some more notations. We denote by $\mathsf{M}_n(\mathbb{Z})$ the set of square matrices of dimension $n \times n$ with integer entries. We define the *conjugacy classes of matrices* $\mathfrak{Cl}(\mathsf{M}_n(\mathbb{Z}))$ as the quotient $\mathsf{M}_n(\mathbb{Z})/\sim$ given by the equivalence relation $M \sim N$ if and only if $M = UNU^{-1}$ for some $U \in \mathsf{GL}_n(\mathbb{Z})$, where $\mathsf{GL}_n(\mathbb{Z})$ denotes the subset of $\mathsf{M}_n(\mathbb{Z})$ of invertible matrices.

For any polynomial f, we denote by $\mathsf{M}_{n,f}(\mathbb{Z})$ the subset of matrices of $\mathsf{M}_n(\mathbb{Z})$ having f as a characteristic polynomial. Since the characteristic polynomial is an invariant of the conjugacy class, then $\mathfrak{Cl}(\mathsf{M}_{n,f}(\mathbb{Z}))$ is well defined.

Let $M \in \mathsf{M}_n(\mathbb{Z})$. Let $\gcd(M)$ be the greatest common divisor of all entries of M. The cofactor $\mathrm{Cof}(M)$ of M is the matrix whose ij-entry is $(-1)^{i+j}$ times the determinant of the matrix that results from the elimination of the i-th row and the j-th column of M. We recall that if M is invertible (over $\mathbb{Q}$), then $M^{-1} = \mathrm{Cof}(M)^t/\det(M)$, where $\mathrm{Cof}(M)^t$ is the transpose of $\mathrm{Cof}(M)$ and $\det(M)$ is the determinant of M. Define the following map

$$\begin{aligned} \tau : \mathsf{M}_n(\mathbb{Z}) &\to \mathbb{Z} \\ M &\mapsto \gcd(\mathrm{Cof}(M)). \end{aligned}$$

Let $M, N \in \mathsf{M}_n(\mathbb{Z})$. We have that $\mathrm{Cof}(MN) = \mathrm{Cof}(M)\,\mathrm{Cof}(N)$ (see for example [1, p. 46, eq. 1.3]). Since $\gcd(M)$ divides every entry of MN, we have that $\gcd(M)|\gcd(MN)$. In particular, $\gcd(MU) = \gcd(UM) = \gcd(M)$ for any $U \in \mathsf{GL}_n(\mathbb{Z})$. Note that $\mathrm{Cof}(U) \in \mathsf{GL}_n(\mathbb{Z})$ if $U \in \mathsf{GL}_n(\mathbb{Z})$. Thus, the map τ induces a map

$$\mathfrak{Cl}(\mathsf{M}_n(\mathbb{Z})) \to \mathbb{Z},$$

which we also denote by τ. We denote by $\mathbf{I}$ the identity matrix. By abuse of language, we write M instead of $[M]$ for the class in $\mathfrak{Cl}(\mathsf{M}_n(\mathbb{Z}))$ of a matrix $M \in \mathsf{M}_n(\mathbb{Z})$.

Statement of the result

We consider an isogeny class $\mathcal{A}$ of g-dimensional ordinary simple abelian varieties defined over a finite field. We denote by $\mathfrak{c}(\mathcal{A})$ the subset of cyclic varieties in the isogeny class $\mathcal{A}$. Our main result states:

Theorem 1. *Let $\mathcal{A}$ be a g-dimensional isogeny class of ordinary simple abelian varieties defined over $\mathbb{F}_q$. Let $f = f_{\mathcal{A}}$ be the Weil polynomial of $\mathcal{A}$. Then there exist bijections between $\mathcal{A}$ (up to $\mathbb{F}_q$-isomorphism) and*

$$\{M \in \mathfrak{Cl}(\mathsf{M}_{2g,f}(\mathbb{Z})) : q^{g-1} | \tau(M)\},$$

and between $\mathfrak{c}(\mathcal{A})$ (up to $\mathbb{F}_q$-isomorphism) and

$$\{M \in \mathfrak{Cl}(\mathsf{M}_{2g,f}(\mathbb{Z})) : q^{g-1} | \tau(M) \text{ and } (\tau(\mathbf{I} - M), \widehat{f(1)}, f'(1)) = 1\}.$$

Here (z_1, z_2, z_3) denotes the greatest common divisor of the integers z_i, $\widehat{z}$ denotes the quotient $z/\operatorname{rad}(z)$ of an integer z to its radical and f' denotes the first derivative of the polynomial f.

3. The proof

The proof uses a version of Deligne's functor and a classical result of Latimer and MacDuffee.

Fractional ideals

Given a number field K, an *order* in K is a subring of K which is finitely generated as a $\mathbb{Z}$-module and such that its fields of fractions equal K. The ring of integers $\mathcal{O}_K$ of K is the maximal order of K. Given an algebraic integer θ, the $\mathbb{Z}$-module $\mathbb{Z}[\theta]$ is an order in $\mathbb{Q}(\theta)$. Given an order $\mathcal{O}$ in a number field K, a *fractional $\mathcal{O}$-ideal* is a nonzero finitely generated sub-$\mathcal{O}$-module of K. Every fractional $\mathcal{O}$-ideal can be written as $\alpha\mathfrak{a}$, where $\mathfrak{a}$ is an (integral) ideal of $\mathcal{O}$ and $\alpha \in K^*$. Given two fractional $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, the product $\mathfrak{ab}$, the sum $\mathfrak{a}+\mathfrak{b}$, the intersection $\mathfrak{a}\cap\mathfrak{b}$, and the ideal quotient

$$(\mathfrak{a} : \mathfrak{b}) := \{\alpha \in K : \alpha\mathfrak{b} \subset \mathfrak{a}\}$$

are fractional $\mathcal{O}$-ideals. Note that if we have orders $\mathcal{O}' \subset \mathcal{O} \subset \mathcal{O}''$ and $\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal, then $\mathfrak{a}$ is a fractional $\mathcal{O}'$-ideal; it is a fractional $\mathcal{O}''$-ideal if $\mathfrak{a}\mathcal{O}'' \subset \mathfrak{a}$, i.e. if it has a module structure over $\mathcal{O}''$. We have that $(\mathfrak{a} : \mathfrak{a})$ is a ring, and it is called the *multiplicator ring of* $\mathfrak{a}$. It is an order in K, and it is the biggest order $\mathcal{O}$ such that $\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal.

We say that two fractional $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* if $\mathfrak{a} = (\alpha\mathcal{O})\mathfrak{b}$ for some $\alpha \in K^*$. The set of equivalence classes is the *ideal class monoid* $\mathrm{ICM}(\mathcal{O})$. It has a monoid structure coming from the multiplication of ideals, which is well defined on the equivalence classes. Note that $(\mathfrak{a} : \mathfrak{a}) = (\mathfrak{b} : \mathfrak{b})$ provided that $\mathfrak{a}$ is equivalent to $\mathfrak{b}$.

Deligne category

By a result of Deligne [2], there exists an equivalence between the category of ordinary abelian varieties over $\mathbb{F}_q$ and modules over $\mathbb{Z}$ with additional structure. Deligne's equivalence is explicit in a convenient way using the language of fractional ideals:

Theorem 2 (Deligne)**.** *Let $\mathcal{A}$ be an ordinary simple isogeny class of abelian varieties defined over $\mathbb{F}_q$, which is defined by the q-Weil polynomial $f_{\mathcal{A}}$. Let α be a root of $f_{\mathcal{A}}$ corresponding to the Frobenius. Then*

1. *we have a bijection between $\mathcal{A}$ (up to $\mathbb{F}_q$-isomorphism) and $\mathrm{ICM}(\mathbb{Z}[\alpha, q/\alpha])$;*
2. *let I_A be the corresponding fractional ideal of an abelian variety $A \in \mathcal{A}$; then $\mathrm{End}_{\mathbb{F}_q}(A)$ corresponds to the multiplicator ring $(I_A : I_A)$.*

Proof. See [8, corollaries 4.4 and 4.6] for this version of Deligne's equivalence. □

Under this bijection, our next goal is to establish a connection between varieties and certain classes of matrices.

Latimer and MacDuffee

The next step is to relate fractional ideals and matrices. This is given by a classical result of Latimer and MacDuffee:

Theorem 3 (Latimer and MacDuffee, see [7])**.** *Let $f(t) \in \mathbb{Z}[t]$ be monic irreducible of degree n, and let α be a root of $f(t)$. Then we have a bijection*

$$\mathrm{ICM}(\mathbb{Z}[\alpha]) \longleftrightarrow \mathfrak{Cl}(\mathsf{M}_{n,f}(\mathbb{Z})). \tag{1}$$

This bijection is given by the following rule. Let $\mathfrak{a}$ be a fractional $\mathbb{Z}[\alpha]$-ideal in $\mathbb{Q}(\alpha)$. Note that multiplication by α is a $\mathbb{Z}$-linear map $m_\alpha : \mathfrak{a} \to \mathfrak{a}$. Then we pick a basis of $\mathfrak{a}$ as a $\mathbb{Z}$-module, and finally we take the matrix that represents the multiplication by α. Changing the basis of the fractional ideal changes this matrix to another in the same conjugacy class. This gives a well-defined function from $\mathrm{ICM}(\mathbb{Z}[\alpha])$ to $\mathfrak{Cl}(\mathsf{M}_{n,f}(\mathbb{Z}))$, which is then independent of the choice of the basis. Theorem 3 states that this function is a bijection. For more details, we refer the reader to the original paper [7], a version given by Taussky in [14], or Conrad notes available online[‡].

We now extend the previous result to the cases interesting to us. In this context, we consider only q-Weil polynomials.

Proposition 1. *Let $f(t) \in \mathbb{Z}[t]$ be an irreducible q-Weil polynomial of degree $n = 2g$, and let α be a root of $f(t)$. Then we have bijections (given by restrictions of bijection of Theorem 3)*

$$\mathrm{ICM}(\mathbb{Z}[\alpha, q/\alpha]) \longleftrightarrow \{M \in \mathfrak{Cl}(\mathsf{M}_{n,f}(\mathbb{Z})) : q^{g-1} | \tau(M)\}, \tag{2}$$

$$\mathrm{ICM}(\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]) \longleftrightarrow \{M \in \mathfrak{Cl}(\mathsf{M}_{n,f}(\mathbb{Z})) : q^{g-1} | \tau(M) \text{ and } \ell | \tau(\mathbf{I} - M)\}, \tag{3}$$

for every prime $\ell | (\widehat{f(1)}, f'(1))$, and where $\sigma_\ell := \frac{f(1)}{\ell(1-\alpha)}$.

Remark 1. *By convention,* $\mathrm{ICM}(\mathcal{O})$ *is empty if $\mathcal{O}$ is not an order. For example, this is the case when $\mathcal{O} = \mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ and σ_ℓ is not an algebraic integer.*

Proof. Since f is a q-Weil polynomial, $\mathbb{Z}[\alpha, q/\alpha]$ is an order in $\mathbb{Q}(\alpha)$ and $\det(M) = f(0) = q^g$ for any matrix $M \in \mathsf{M}_{n,f}(\mathbb{Z})$. We consider bijection (1) of Theorem 3. Let $\mathfrak{a}$ be a fractional $\mathbb{Z}[\alpha]$-ideal. If $M \in \mathsf{M}_{n,f}(\mathbb{Z})$ represents multiplication by α on the fractional ideal $\mathfrak{a}$ for some choice of $\mathbb{Z}$-basis, then $qM^{-1} \in \mathsf{M}_n(\mathbb{Q})$ represents multiplication by $q\alpha^{-1}$ on $\mathbb{Q}(\alpha)$ for the same basis, as a $\mathbb{Q}$-linear map. Here, the inverse matrix M^{-1} exists since its determinant is different from zero. The fractional $\mathbb{Z}[\alpha]$-ideal $\mathfrak{a}$ has a module structure over the order $\mathbb{Z}[\alpha, q/\alpha]$ if and only if multiplication by $q\alpha^{-1}$ is well defined in $\mathfrak{a}$ as a $\mathbb{Z}$-linear map, that is, $qM^{-1} \in \mathsf{M}_n(\mathbb{Z})$. Then bijection (2) follows from

$$qM^{-1} = q\frac{\mathrm{Cof}(M)^t}{\det(M)} = \frac{\mathrm{Cof}(M)^t}{q^{g-1}},$$

[‡]https://kconrad.math.uconn.edu/blurbs/

and the definition of τ.

The $\mathbb{Z}$-module $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ is an order if and only if σ_ℓ is an algebraic integer. We now compute the characteristic polynomial of σ_ℓ. Let us denote by p_θ the characteristic polynomial of any algebraic number θ in $\mathbb{Q}(\alpha)$. Observe that $\theta, 1-\theta, \theta^{-1}$ and $c\theta$ ($c \in \mathbb{Q}^*$) have the same degree. Let $p_\alpha(t) = \sum_{i=0}^n a_i t^i \in \mathbb{Z}[t]$ and $p_\beta(t) = \sum_{i=0}^n b_i t^i \in \mathbb{Z}[t]$ be the characteristic polynomials of α and $\beta := 1-\alpha$, respectively. Then $\sum_{i=0}^n \frac{b_{n-i}}{b_0} t^i \in \mathbb{Q}[t]$ is the characteristic polynomial $p_{\beta^{-1}}$ of β^{-1} since it is monic and equals zero when evaluated at β^{-1}. By similar arguments, we have that $p_{c\beta^{-1}}(t) = \sum_{i=0}^n c^{n-i} \frac{b_{n-i}}{b_0} t^i$. If we take $c := \frac{b_0}{\ell}$, we have

$$p_{c\beta^{-1}}(t) = \sum_{i=0}^{n} \frac{b_0^{n-i-1}}{\ell^{n-i}} b_{n-i} t^i = t^n + \frac{1}{\ell} b_1 t^{n-1} + \frac{b_0}{\ell^2} b_2 t^{n-2} + \cdots + \frac{b_0^{n-2}}{\ell^{n-1}} b_{n-1} t + \frac{b_0^{n-1}}{\ell^n}.$$

By comparing the following identity (the coefficients of β^i have to be the same)

$$0 = p_\beta(\beta) = \sum_{i=0}^{n} b_i \beta^i = \sum_{i=0}^{n} a_i (1-\beta)^i,$$

we get $b_0 = \sum_{i=0}^n a_i = f(1)$ and $b_1 = -\sum_{i=0}^n i a_i = -f'(1)$. Finally, the characteristic polynomial of σ_ℓ has all its non-leading coefficients of the form $\frac{f(1)^{i-1}}{\ell^i}$ times an integer, except for the coefficient of degree $n-1$, which equals $-\frac{f'(1)}{\ell}$, and that the constant term equals $\frac{f(1)^{n-1}}{\ell^n}$. Thus, $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ is an order if and only if $\ell | (\widehat{f(1)}, f'(1))$.

Let $\mathfrak{a}$ be a fractional $\mathbb{Z}[\alpha, q/\alpha]$-ideal. As in the previous case, if $M \in \mathsf{M}_{n,f}(\mathbb{Z})$ represents multiplication by α on the fractional ideal $\mathfrak{a}$ for some choice of $\mathbb{Z}$-basis, then $(f(1)/\ell)(\mathbf{I}-M)^{-1} \in \mathsf{M}_n(\mathbb{Q})$ represents multiplication by $(f(1)/\ell)(1-\alpha)^{-1}$ on $\mathbb{Q}(\alpha)$ for the same basis, as a $\mathbb{Q}$-linear map. Note that $\det(\mathbf{I}-M) = f(1) \neq 0$. Provided that $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ is an order, the fractional ideal $\mathfrak{a}$ has a module structure over the order $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ if and only if multiplication by σ_ℓ is well defined in $\mathfrak{a}$ as a $\mathbb{Z}$-linear map, that is,

$$\frac{f(1)}{\ell}(1-M)^{-1} = \frac{f(1)}{\ell} \frac{\mathrm{Cof}(\mathbf{I}-M)^t}{\det(\mathbf{I}-M)} = \frac{\mathrm{Cof}(\mathbf{I}-M)^t}{\ell} \in \mathsf{M}_n(\mathbb{Z}).$$

Then bijection (3) follows from the definition of τ. □

Proof of Theorem 1

The first bijection follows immediately from bijection (2) of Proposition 1 and the first bijection of Theorem 2 (Deligne's equivalence).

Now, for $A \in \mathcal{A}$, denote by I_A its associated fractional ideal (from Theorem 2), and by M_A the class of matrices associated to I_A (from Theorem 3). From Lemma 2.1 of [4], the variety A is cyclic if and only if, for each prime $\ell | f(1)$, there is no endomorphism $\varphi \in \mathrm{End}_{\mathbb{F}_q}(A)$ such that $\varphi \circ [\ell] \circ (1-F) = [f(1)]$, where $[z] \in \mathrm{End}_{\mathbb{F}_q}(A)$

denotes multiplication by an integer z and $\circ$ the composition of morphisms. From part 2 of Theorem 2, the latter is equivalent to

$$\sigma_\ell := \frac{f(1)}{\ell(1-\alpha)} \notin (I_A : I_A),$$

for each prime $\ell | f(1)$, and where the Frobenius F is represented by a fixed root α of f. We recall (see the proof of Proposition 1) that for each prime $\ell | f(1)$ such that $\ell \nmid (\widehat{f(1)}, f'(1))$, we have automatically that $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell] \not\subset (I_A : I_A)$ since $\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell]$ is not an order. Thus, A is cyclic if and only if

$$\mathbb{Z}[\alpha, q/\alpha, \sigma_\ell] \not\subset (I_A : I_A),$$

for each prime $\ell | (\widehat{f(1)}, f'(1))$. Finally, from bijection (3) of Proposition 1, the latter is equivalent to

$$q^{g-1} | \tau(M_A) \text{ and } (\tau(\mathbf{I} - M_A), \widehat{f(1)}, f'(1)) = 1.$$

The result follows.

Acknowledgement

This work is part of my PhD dissertation. I would like to thank my advisor Serge Vlăduţ for very fruitful discussions and for his very useful comments and suggestions. I would also like to thank the anonymous reviewers for their valuable remarks, which helped to improve the manuscript substantially.

References

[1] S. J. Beslin, *Cofactor matrices*, Linear Algebra Appl. **165**(1992), 45–52.
[2] P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8**(1969), 238–243.
[3] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, available at `http://www.lmfdb.org`.
[4] A. J. Giangreco-Maidana, *On the cyclicity of the rational points group of abelian varieties over finite fields*, Finite Fields Appl. **57**(2019), 139–155.
[5] A. J. Giangreco-Maidana, *Local cyclicity of isogeny classes of abelian varieties defined over finite fields*, Finite Fields Appl. **62**(2020), Article 101628.
[6] E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347**(1995), 2361–2401.
[7] C. G. Latimer, C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. **34**(1933), 313–316.
[8] S. Marseglia, *Computing square-free polarized abelian varieties over finite fields*, Math. Comp. **90**(2021), 953–971.
[9] D. Mumford, *Abelian varieties*, vol. 5 of Tata Institute of Fundamental Research Studies in mathematics, Oxford University Press, Oxford, 1970.
[10] H. -G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49**(1987), 301–304.

[11] S. RYBAKOV, *The groups of points on abelian varieties over finite fields*, Cent. Eur. J. Math. **8**(2010), 282–288.
[12] R. SCHOOF, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46**(1987), 183–211.
[13] J. TATE, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2**(1966), 134–144.
[14] O. TAUSSKY, *On a theorem of Latimer and MacDuffee*, Canad. J. Math. **1**(1949), 300–302.
[15] M. A. TSFASMAN, *Group of points of an elliptic curve over a finite field*, in: *Theory of numbers and its applications*, Tbilisi, 1985, 286–287.
[16] S. G. VLĂDUŢ, *Cyclicity statistics for elliptic curves over finite fields*, Finite Fields Appl. **5**(1999), 13–25.
[17] S. G. VLĂDUŢ, *On the cyclicity of elliptic curves over finite field extensions*, Finite Fields Appl. **5**(1999), 354–363.
[18] J. F. VOLOCH, *A note on elliptic curves over finite fields*, Bull. Soc. Math. Fr. **116**(1988), 455–458.
[19] W. C. WATERHOUSE, *Abelian varieties over finite fields*, Ann. Sci. Éc. Norm. Supér. **2**(1969), 521–560.